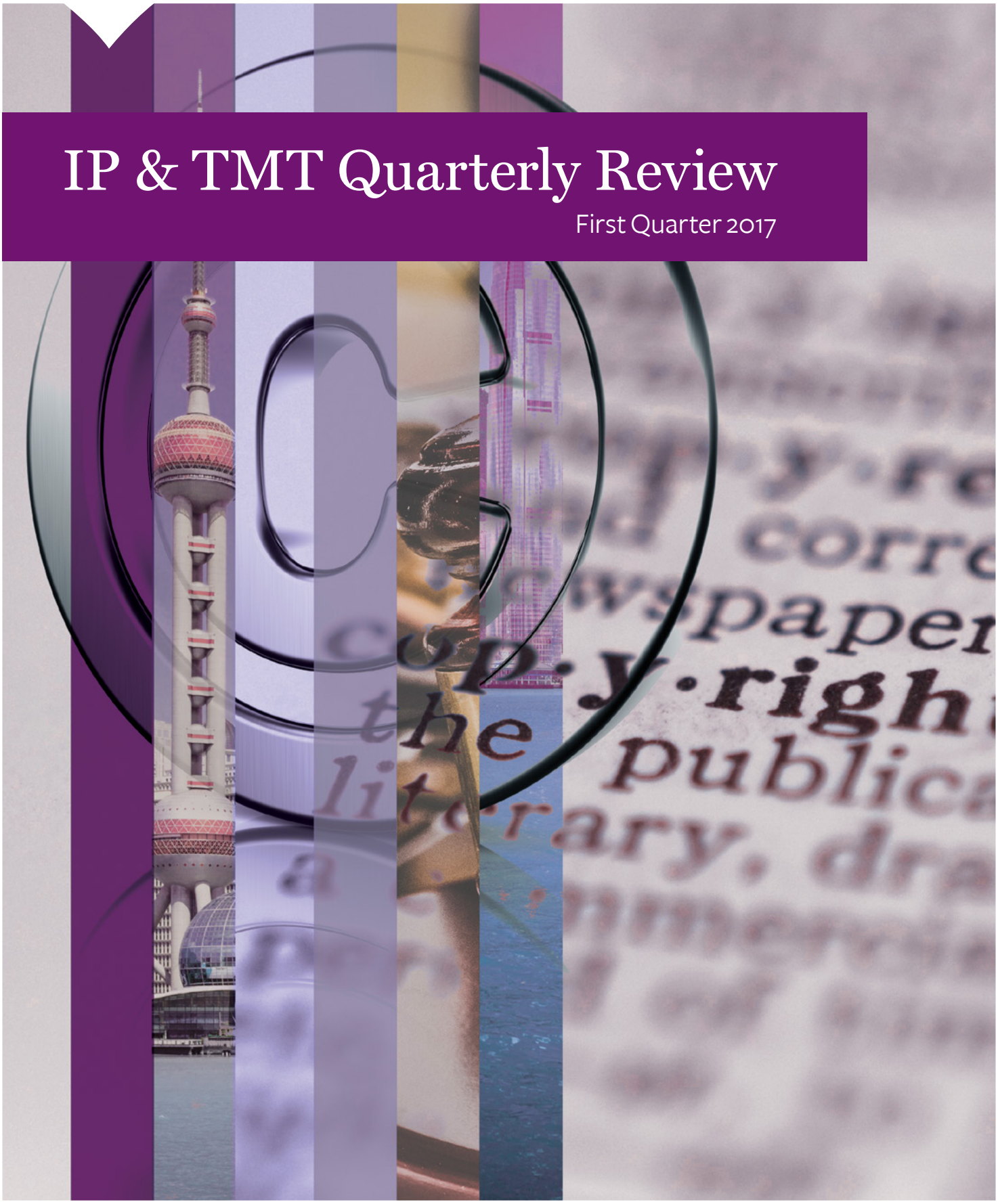
MAYER·BROWN
JSM

IP & TMT Quarterly Review

First Quarter 2017



www.mayerbrownjsm.com

Content

Key: Click to Navigate

CHINA

Trade Marks

By Benjamin Choi, Partner, Mayer Brown JSM, Hong Kong

Michael Jordan: "Qiao Dan" is Me!

Michael Jordan, the legendary NBA star, has finally established his rights in his Chinese name after 5 years of intensive administrative and appeal proceedings in China.

In China, Jordan is more commonly known and addressed by the Chinese name "乔丹" (pronounced as "Qiao Dan" in Mandarin) which resembles the pronunciation of "Jordan". This is another typical case of a foreign brand owner's Chinese name being hijacked by a PRC entity. The hijacker had a real business which used both "乔丹" and "QIAODAN" as trade marks on shirts, sport shoes and apparel manufactured and sold in China since 2000. Michael Jordan had a long and hard fight to get his name back. He is now half way through recovering the "乔丹" trade mark, whilst the "QIAODAN" trade mark is still in somebody else's hands.

Facts and Rulings

From 2000 onwards, Qiaodan Sports Co. Ltd. ("**Qiaodan Sports**") registered a number of trade marks including "乔丹", "QIAODAN" and a logo resembling the famous "Jumpman Logo" of Michael Jordan.

In 2012, Michael Jordan sued Qiaodan Sports for infringement of his name rights in China. He asked the Chinese authorities to invalidate the registered marks of Qiaodan Sports, on the basis that they had the potential to mislead consumers that the goods of Qiaodan Sports are associated or otherwise authorized by Michael Jordan.

The Trademark Review and Adjudication Board, the Beijing No. 1 Intermediate People's Court and the Beijing High Court consistently came to the view that "Jordan" is a common American surname which is not readily and uniquely associated with Michael Jordan. The lower courts also perceived no exclusive and definitive link between Michael Jordan and "乔丹"/"QIAODAN", but commercially this is clearly not

the case. Michael Jordan decided to recover the valuable commercial rights in his name by appealing to the Supreme People's Court ("**SPC**").

Favourable Decision - "乔丹"

Michael Jordan successfully demonstrated that "乔丹" is well-recognized in China and clearly associated with Michael Jordan personally. The SPC recognized an *established link* between "乔丹" and Michael Jordan, and that Qiaodan Sports had "malicious intent" in registering "乔丹" as a trade mark when it was fully aware of Michael Jordan's reputation in China. Therefore, use of "乔丹" by Qiaodan Sports infringed upon Michael Jordan's prior rights in his name and the SPC ordered the "乔丹" trade mark registration to be invalidated.

Unfavourable Decision - "QIAODAN"

"QIAODAN" is the English transliteration of "乔丹". The meanings of "QIAODAN" and "乔丹" are identical, but from the perspective of trade mark use, the SPC could not find an established link between "QIAODAN" and Michael Jordan, as naturally Michael Jordan would not have used "QIAODAN" in any manner. The SPC therefore concurred with the lower courts' decisions in the invalidation actions against "QIAODAN" and related formative marks in favour of Qiaodan Sports.

Conclusion and Recommendations

Michael Jordan's success in recovering his Chinese name "乔丹" serves as an encouraging precedent to brand owners.

At least the SPC is seen to have considered all relevant circumstances, in particular the fairness and commercial value behind the name, in order to reach a finding that Michael Jordan can have his long lost Chinese name back as a trade mark that is likely to be worth millions of dollars.

The applicable laws and provisions have not changed. The Chinese authorities and courts are willing to see and listen. The key to success is for the foreign brand or name owners to present sufficient evidence to support their rights and show bad faith on the part of the trade mark squatter. There is no other magic involved.

Michael Jordan's case and other similar cases involving brand owners such as New Balance and Hermès, emphasise the need for foreign brand owners to identify and register a Chinese version of their brands be it as a translation or as a transliteration as soon as possible, in order to ensure that they are protected against trade mark squatters. ◆

CHINA

Trade Marks

By Rosita Li, Partner, Mayer Brown JSM, Hong Kong

Statutory Damages for Trade Mark Infringement and/or Under the Anti-Unfair Competition Law ("AUCL"): A New Normal?

The PRC courts' determination to enhance protection for proprietors of trade marks and trade dress is reflected in recent decisions in trademark infringement and unfair competition cases. Damages awarded under AUCL are calculated by reference to the methods for calculating damages under the Trademark Law, applying the same factors. The upper limit of statutory damages under the PRC Trademark Law was increased from RMB 500,000 to RMB 3 million in 2014. Since this amendment to the PRC Trademark Law, we have noticed a trend for the PRC courts to exercise their discretion and award maximum or near-maximum statutory damages in claims for trade mark infringement, and also for claims under the AUCL.

In the last quarter of 2015, the Beijing IP court awarded its first maximum statutory damages to Moncler, a foreign plaintiff which took action against Nuoyakate for trademark infringement and unfair competition. The Beijing IP court issued a judgment against Nuoyakate for trade mark infringement and unfair competition and awarded Moncler an unprecedented high amount of damages. For details of the Moncler case and our comments, please see our article in a previous issue of the IP/TMT Quarterly Review.

Since the Moncler case, the PRC courts have awarded the maximum/near-maximum amount of statutory damages in other cases involving both local and foreign plaintiffs thus proving that the Moncler case was not an isolated case.

In September 2016, in a claim for trade mark infringement and unfair competition, BMW was also awarded RMB3 million damages in respect of its claim against a Defendant who manufactured and sold products with a logo similar to BMW's logo and used the "BMN" trading name. The Defendant in the BMW

case had over 400 stores in China and the infringing activities lasted for 7 years.

Early this year, in a claim for unfair competition under AUCL the court held that the Defendant's trade dress for its cocktail products bearing the BIO mark was almost the same as the Plaintiff's famous and unique trade dress for its RIO cocktail products and the Defendant's action amounted to unfair competition under AUCL. The Defendant was ordered to pay the Plaintiff RMB3 million damages and RMB4,200 reasonable expenses.

In the unfair competition dispute between "QQ Star" of Yili and "Future Star" of Mengniu where both the Plaintiff and the Defendant manufactured and sold dairy products targeting children, the court held in February 2017 that the Defendant's product packaging was similar to the packaging for the Plaintiff's products and found in favour of the Plaintiff under AUCL. The court awarded the Plaintiff RMB2.15million damages.

When considering the amount of damages that should be awarded, the court will look at the following:-

1. The level of actual losses suffered by the Plaintiff;
2. If the above is difficult to determine, the amount of profits gained by the Defendant;
3. If the above is difficult to determine, the amount of royalty fee paid for the use of the trademark concerned;
4. If the infringement is serious, the court may order punitive damages of up to three times of the damages calculated by one of the above methods; or
5. (a) If all of the above methods are difficult to determine; or
   (b) The Plaintiff has done as much as practically possible in providing evidence, has proven that the relevant financial recordings are held by the Defendant but the Defendant refused to provide such evidence, the courts may grant discretionary statutory damages based on the evidence provided by the Plaintiff.

In most of the cases highlighted in this article, the PRC courts granted discretionary statutory damages because it was difficult to assess the actual loss or profits, or the infringers refused to provide their accounting records.

There are no explicit guidelines on how to calculate the amount of damages. In the recent PRC cases where near maximum statutory damages were awarded, the courts considered similar factors, namely, the scale of infringement, geographical span of the infringing activities, the reputation of the plaintiffs and the duration of the infringing activities. It is important to note that the PRC courts also emphasized in all the abovementioned cases that the malicious intent of the defendants is a major factor that is taken into account when awarding statutory damages in the upper range.

The court's continued willingness to award maximum statutory damages in claims under the Trademark Law and the AUCL will hopefully have a deterrent effect on infringers. The two recent decisions under AUCL provide an indication that the PRC courts are more ready to protect trade dress under AUCL. This is certainly good news for rights owners. Nevertheless, it is still advisable for rights owners to register the specific elements that make up trade dress and which are registrable e.g. trademarks, or copyright to obtain better protection for their rights. ◆

HONG KONG

Patents

By Amita Kaur Haylock, Senior Associate, Mayer Brown JSM, Hong Kong

Interlocutory Injunctions - Inordinate Delay can be Damaging

In a recent case, *Xcelom Limited v BGI-Hong Kong Co. Limited* [2016] *HKEC 2061*, the Plaintiffs' application for an interlocutory injunction to restrain the Defendants from using or offering for use in Hong Kong a non-invasive prenatal test for screening of chromosomal aneuploidies, was denied due to the delay by the Plaintiffs in commencing proceedings against the Defendants.

Background

The case concerned a patent granted in Hong Kong in 2014 (based on a European Patent) for the non-invasive prenatal test named NIFTY. Sometime in January 2015, the Plaintiffs became aware that the Defendants were also providing non-invasive prenatal testing services in Hong Kong under the name "NIFTY", and which could achieve results identical to the Plaintiffs' own NIFTY technology and was therefore infringing the Plaintiffs' patent. However, the Plaintiffs did not commence legal proceedings against the Defendants until more than 11 months later in December 2015 when they also issued an *inter partes* summons for an interlocutory injunction.

Judgment

The Plaintiffs argued that there was no undue delay as in March 2015, they attempted to warn people (presumably that the Defendants' "NIFTY" test was infringing the Plaintiffs' patent), in June 2015, they sent a cease and desist letter to the Defendants, and between August to October 2015, they were in talks with the Defendants.

The judge rejected these contentions on the basis that they did not explain the delay which was *inordinate*. Instead of moving with due diligence to seek an injunction immediately, the Plaintiffs took almost a year to issue proceedings, which is not characteristic of persons suffering irreparable damage.

The Plaintiffs also argued that the strength of their case was relevant when deciding if the interlocutory injunction should be granted (relying on *Series 5 Software Ltd v Philip Clarke & Others [1996] FSR 273*). This was again rejected by the court. It was not part of the court's function at the interlocutory stage to try to resolve conflicts of evidence on affidavit as to facts on which the claims of either party may ultimately depend. Nor should the court decide difficult questions of law which should be dealt with at trial (relying on the House of Lords decision in *American Cyanamid Co v Ethicon Ltd [1975] AC 396*). The court further held that the strength of a plaintiff's case is not relevant beyond whether there is a serious issue to be tried. The other principles governing the grant or refusal of an interlocutory injunction are irreparable harm/ inadequacy of damages in the event the plaintiff succeeds at trial, if the balance of convenience lies in favour of granting the injunction and if the plaintiff can provide an undertaking to pay damages to the defendant for any loss sustained by reason of the injunction if it subsequently transpires that the injunction should not be granted.

The Plaintiffs' interlocutory injunction application was therefore dismissed.

Conclusion

The key question as regards inordinate delay is whether a plaintiff's delay was considered reasonable under the circumstances of the case. Although it is important to act quickly when faced with evidence of possible infringement, for example by promptly sending a cease and desist letter, certain delays are understandable and likely to be excused by the courts. A delay in applying for an injunction may be justified when it results, for example, from a plaintiff's good faith efforts to investigate the alleged infringement.

The Plaintiffs in Xcelom took around five months from the time they were first made aware of the Defendants' marketing activities to issue a cease and desists letter. They then took another six months to issue the writ and summons for the interlocutory injunction (which were issued on the same day). The court rejected the Plaintiffs' contention that they had to consider the costs of litigation (amongst other things) after sending the cease and desist letter in June before commencing proceedings in December of the same year. ◆

CHINA

Patents

By Xiaoyan Zhang, Counsel, Mayer Brown JSM, Shanghai

GPNE vs. Apple: A Tale of 129 Million Dollars

On 28 January 2013, Hawaii-based GPNE Corporation, a non-practicing entity ("**NPE**"), sued Apple and several other companies in Shenzhen, China, alleging, *inter alia*, that Apple's iPhone and iPad products infringed GPNE's Chinese patent on a paging method and device (the "**Patent**"). This infringement case is one of several global patent disputes initiated by GNPE concerning their wireless patent family. On 28 November 2016, GPNE raised its damages demand in the Shenzhen case from USD ~14 M to ~129 M, making this the largest damages claim in Chinese IP history to date.

Facts & Arguments

The Patent, issued in 2001 and expired in 2015, concerns a two-way paging system utilizing four local frequencies for transmitting signals between a pager and a central control station. GPNE has asserted that the Patent covers the basic 3GPP communication standard commonly used by the General Packet Radio Services ("**GPRS**") and patent protection has been awarded for this technology in 13 countries in addition to China. Consequently, GPNE alleges that any devices with the GPRS function including mobile phones and tablet PCs, fall within the scope of the Patent. Apple, on the other hand, contends that the Patent is limited to pagers and does not cover Apple's iPhone or iPad products. The case is currently pending before the Shenzhen Intermediate People's Court after three trials.

History of the Case

In parallel to the infringement case in Shenzhen, Apple and others have challenged the validity of the Patent before the Patent Re-examination Board ("**PRB**") in Beijing. The Patent, however, survived all five challenges. In 2014 Apple appealed the PRB decision to the Beijing First Intermediate People's Court, which then rejected Apple's arguments and affirmed the validity of the Patent.

In the infringement case, the Shenzhen Intermediate People's Court appointed the Centre for Identification of Intellectual Property of Ministry of Industry and Information Technology Institute (the "**Centre**") to undertake a technical appraisal of the Patent. The Centre issued an opinion on 15 July 2016, rejecting Apple's argument that the Patent excludes mobile phones or tablet PCs, and concluding instead that the Patent covers all essential technical characteristics of the GPRS standard.

Notably, separate from the Shenzhen case, GPNE had sued Motorola, Cisco, Blackberry, Samsung, LG, Sony Ericsson, Sharp, HTC and many other well-known mobile communications equipment providers, in the United States where patent damages are typically higher than in other jurisdictions. Most of these lawsuits led to either a global settlement or a patent licensing agreement. In China, GPNE has entered into a patent licensing agreement with Huawei and Microsoft, respectively.

China as a Venue for Global Patent Enforcement

The fact that an NPE now chooses China as a jurisdiction for strategic patent enforcement is interesting. Historically, foreign companies have been sceptical about the adequacy and efficacy of the Chinese patent litigation system. One looming obstacle has been the lack of discovery in litigation, which, when coupled with the heavier burden of proof placed on the plaintiff, renders the proof of actual damages effectively impossible. Thus, an overwhelming majority of the patent infringement cases in China resulted in awards of statutory damages, which are capped at RMB 1M (USD ~145K). The latest draft of the Fourth Amendment to China's Patent Law (the "Fourth Amendment") increases the statutory damages to RMB 5M (USD ~724K) and, proposes other solutions to address the efficacy of the system by empowering Chinese courts to compel discovery in respect of damages as well as the discretion to double or treble patent damages upon a finding of intentional infringement. The Fourth Amendment to China's Patent Law is expected to go into effect later this year.

Under the current Chinese patent enforcement system, GPNE bears the burden to prove the damages it seeks with little aid from discovery in China. Indeed, GPNE appears to have relied on publicly available financial information to come up with its estimation of damages. The high damages demand is, in part, due to the large quantity of Apple products sold to Chinese consumers.

The limitation period for the commencement of a patent infringement action in China is two years. Time starts to run from the date when the plaintiff became or should have become aware of the infringement. Where a plaintiff files a lawsuit after the two-year limitation period, and the infringement remains ongoing when the case is filed, the people's court will order the defendant to cease the infringing acts during the period of patent validity, and the amount of patent damages will be calculated over a period of two years counting backwards from the date on which the plaintiff filed the case.

Although the Patent expired in 2015 in the present case, GPNE can still demand damages in the amount of illegal profits earned by Apple over a period of two years counting backwards from the date on which GPNE filed its complaint. Since Apple is a publicly listed company, GPNE can rely on Apple's published annual financial reports to calculate the illegal profits earned from the alleged infringement. As the relevant profits are USD ~7.69B for mobile phones and ~1.79B for tablets, GPNE can in theory demand USD ~9B patent damages for both infringing products. In Chinese courts, however, a plaintiff's litigation costs payable rise as its damages demands increase pursuant to the *PRC Litigation Costs Payment Guidelines*. A demand of USD ~9B damages would result in the litigation costs payable by GPNE of USD ~4.8M. The final USD 129M damages demand thus likely reflects GPNE's compromise taking into account affordable litigation costs.

Patents Cont'd

Conclusion

The outcome of the Shenzhen case is anybody's guess. Most likely, Apple and GPNE will reach a settlement agreement considering the large demand for damages at stake. This case might well mark a new era where China joins the US and other major jurisdictions as a potential global patent enforcement venue for NPEs and other patent rights holders. When the more plaintiff-friendly damages rules are enacted once the Fourth Amendment to China's Patent Law is finalised, patent infringement cases in China will likely shift from targeting public companies with a large consumer base such as the case here, to other types of companies as well. ◆

HONG KONG

Data Privacy

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.F. Lee, Senior Associate, Mayer Brown JSM, Hong Kong

Do Not Disturb! Convictions for Breach of the Direct Marketing Restrictions and Unsolicited Electronic Messages Ordinance

On 10 January 2017, an individual was convicted of 3 offences for breach of an enforcement notice issued against him for sending commercial electronic messages in violation of the Unsolicited Electronic Messages Ordinance (Cap.593) ("**UEMO**"). Soon after, on 27 January 2017, the High Court upheld the Tsuen Wan Magistrates' Court's landmark conviction of 2015 in which the internet service provider, Hong Kong Broadband Network Limited ("**HKBN**"), was fined HK$30,000 for breach of the direct marketing provisions under the Personal Data (Privacy) Ordinance ("**PDPO**").

The Law

Under the PDPO, data users cannot use personal data for direct marketing purposes unless they obtain the prior consent of the relevant individual. Even after consent is provided, the individual has the right to opt-out, and the data user must promptly comply with such opt-out request and cease providing direct marketing materials. A breach of the direct marketing restrictions under the PDPO amounts to an offence, and can result in a maximum fine of HK$ 500,000 and 3 years imprisonment. If there has been a transfer in return for gain of personal data for direct marketing purposes, then a higher fine of HK$ 1,000,000 and up to 5 years imprisonment may be imposed.

The direct marketing restrictions under the PDPO only apply to the use of personal data collected by a data user to send marketing materials to a specific person. For example, a company using the personal data collected by it in order to send a promotional text message to the relevant individual and identifying them by name. In contrast, if a company sends text messages to a random telephone number, not knowing or being able to identify the recipient, then this may not fall

Data Privacy Cont'd

within the scope of the PDPO. However, such unsolicited marketing messages may still fall foul of the UEMO.

The UEMO regulates the sending of marketing or promotional electronic messages (i.e. spam). Whilst it regulates pre-recorded telephone messages, text messages, facsimiles and emails, it does not apply to person-to-person calls or other non-electronic messages. Ongoing proposals to expand the UEMO to include person-to-person calls have so far not been effective[1].

Under the UEMO, consumers can register their telephone or fax numbers on a do-not-call register (administered by the Office of the Communications Authority). Any business that sends unsolicited commercial electronic messages to a number which is registered on the do-not-call register, without the consent of the recipient, is in breach of the UEMO. For any other telephone or fax numbers not registered on the do-not-call register, businesses can send them commercial electronic messages, so long as certain requirements are complied with. For example:

- The sender must clearly identify itself and provide contact information in the electronic message;
- The sender must offer a way for the recipients to unsubscribe and to notify the recipient of how they can exercise this right; and
- The sender must comply with any unsubscribe request within 10 working days.

If there is a breach of the UEMO, the Communications Authority ("**CA**") can issue an enforcement notice against the infringer requiring them to take specified steps to rectify the contravention within a reasonable period of time. Anyone who contravenes an enforcement notice will be liable to a fine of HK$100,000 or, on a second or subsequent conviction, to a fine of HK$500,000 (and a further daily fine of HK$1,000 for each day that the offence continues).

The PDPO Case

Despite having opted out of receiving direct marketing messages from HKBN, in May 2013 the complainant received a voice message from HKBN reminding the complainant that his service contract was coming to an end, and further promoting HKBN's services. On 9 September 2015, the lower court held that such a telephone call amounted to direct marketing and therefore breached the direct marketing restrictions under the PDPO. HKBN was fined HK$ 30,000. The lower court's decision was the first conviction issued after the new direct marketing provisions came into effect on 1 April 2013[2].

HKBN filed an appeal on the grounds that the lower court had erred in finding that the telephone call amounted to direct marketing, rather than a notice informing the complainant of the upcoming termination of his service contract.

On appeal, the High Court upheld the lower court's finding that the telephone call provided information to the complainant on an early renewal promotion, and therefore amounted to direct marketing. The High Court confirmed that the definition of "directing marketing" under the PDPO is to be interpreted broadly, so as to include any offer or promotion of goods, services or other business opportunities, even if disguised as purely informational. Financial loss or other harm does not need to have been suffered by the complainant in order for the Privacy Commissioner and Department of Justice to take enforcement action against a breach of the direct marketing provisions.

The UEMO Case

An individual ("**Sender**") had sent unsolicited fax messages promoting their design and decoration services to various third parties. The fax messages did not contain the Sender's name or address. The Sender also failed to comply with requests from recipients to

1 See our article entitled "Call Me Maybe? Hong Kong Privacy Commissioner Proposes Expansion of the Do-Not-Call Register"

2 See our article entitled "Two Companies Convicted for Breach of the Direct Marketing Provisions under the Hong Kong Personal Data (Privacy) Ordinance"

unsubscribe them from the Sender's list for such unsolicited facsimile messages, and he had disconnected the unsubscribe facility so that recipients could not send him opt-out requests.

In October 2015, following several complaints, the CA issued an enforcement notice against the Sender requiring him to stop sending commercial facsimile messages in breach of the UEMO. However, despite the enforcement notice, the CA continued to receive complaints from the public in relation to the Sender.

On 10 January 2017, the Sender was convicted by the West Kowloon Magistrates' Courts for failing to comply with an enforcement notice, and fined HK$7,500. He was also ordered to pay HK$60,000 to the CA to cover the CA's investigation costs and expenses.

More to Follow?

In 2016, the Privacy Commissioner received 393 complaints relating to the direct marketing restrictions under the PDPO – a 22% increase compared to 2015[3].

Since the new direct marketing provisions came into effect on 1 April 2013, there have been 7 convictions for breach of the direct marketing requirements. The highest penalty so far has been the HK$ 30,000 fine issued against HKBN. Whilst the fines imposed to date have been relatively low, the courts have taken a strict approach to the enforcement of the PDPO and have demonstrated that they are willing to interpret the direct marketing provisions broadly. No one is beyond the reach of the courts. Even individuals[4] and outsourced service providers [5] have been held accountable.

In comparison, this latest conviction under the UEMO is only the second time that a person has been found guilty of breach of the UEMO. Despite the rarity of convictions under the UEMO, this latest case may be a kick start to further prosecutions in the future, with the CA being spurred on and inspired by the increasing stream of convictions under the PDPO.

Takeaway Points

Do reminders of renewals of contracts amount to direct marketing? The recent High Court's decision in the HKBN appeal, re-affirms the fact that notifying a customer of the upcoming expiry of their service contract may amount to direct marketing if the data user offers further deals or provides information on their services. Unless such marketing has been consented to by the data subject, the notification could amount to a breach of the PDPO. Data users who use staff to "market" the renewal of contracts should review their privacy policies, personal information collection statements and other records regarding consent to direct marketing. They should provide ongoing training of staff and regularly review their telephone scripts and email templates to ensure that there is no "hidden" marketing that may fall foul of the PDPO.

In addition, companies who are not caught by the PDPO must remember that the UEMO still regulates the sending of any promotional electronic messages. In particular, they should ensure that they include their contact details in all unsolicited electronic messages, and should promptly cease to send any further messages to any individuals who have requested to opt-out of receiving them. Failure to comply with the UEMO and any subsequent enforcement notice can result in not only a fine, but the reimbursement of the CA's expenses incurred as a result of the investigation (which may be significant). ◆

3 https://www.pcpd.org.hk/english/news_events/media_statements/press_20170124b.html

4 See our article entitled " How Much is that Data in the Window? Individual Convicted for Transferring Personal Data to Third Party for Direct Marketing Purposes"

5 See our article entitled "To Market or Not to Market? Outsourced Service Provider Convicted for Breach of Direct Marketing Provisions"

HONG KONG

Data Privacy

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Karen H.F. Lee, Senior Associate, Mayer Brown JSM, Hong Kong

IoT (I Own Thee): Hong Kong Releases Results of Study on Wearable Technology Devices

In January 2017, the Hong Kong Privacy Commissioner ("**PC**") announced the results of the Hong Kong study of the privacy and security practices and protection measures of manufacturers of wearable technology devices, such as fitness bands.

Wearable technologies are a subset of the Internet of Things ("**IoT**"). They are networked devices which collect vast amounts of data, can track activities and behaviours, and enhance and customise users' experiences. Their popularity is on the rise. But how transparent are the manufacturers of the wearable technologies regarding their collection and use of personal data? This was the question raised as part of the 2016 Global Privacy Enforcement Network Sweep ("**Global Sweep**"), in which 25 privacy enforcement authorities (including those in Hong Kong, Canada, the UK and Australia) carried out a review.

The Study

During April to June 2016, the PC carried out a study on five Hong Kong-manufactured fitness bands and their related mobile applications. For the purposes of benchmarking, the PC also examined a popular US-manufactured fitness band.

The main aim of the study was to determine the privacy challenges and implications presented by both fitness bands and IoT devices in general, and to raise the awareness of manufacturers on their obligations under the Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**").

Collectively, 314 IoT devices were globally examined as part of the Sweep by the PC and 24 other privacy enforcement authorities. The majority were medical or health related devices (e.g. monitoring sleep and blood pressure) and fitness wearables.

On 24 January 2017, the PC announced the results of the study.

Key Findings

The PC found that only two out of the five manufacturers in Hong Kong (i.e. 40%) provided their users with a privacy policy on how their personal data would be handled. However, only one of those policies was specifically in relation to the fitness device and set out the types of personal data collected and how it was collected. The other privacy policy was a general one that related to the collection of personal data by the manufacturer's website, and did not address how or what type of personal data was collected by the relevant fitness band.

The results of the study in Hong Kong were consistent with the findings of the other 24 privacy enforcement authorities. In short, 59% of the IoT devices examined globally did not provide specific privacy policies tailored to the relevant device, which sufficiently informed users on how their personal data would be collected, used and disclosed.

The PC also found that all five of the Hong Kong-manufacturers examined, required users to not only provide personal data during registration on the related mobile application, but also obtained access to other functions and data on the users' smartphones (e.g. location data, photo albums, social media accounts, camera, etc). Concerns were raised by the PC and other privacy enforcement authorities as to whether or not all of the data being collected by the IoT devices was actually necessary. The PC also noted an inconsistency in the default access settings of the mobile applications, depending on whether or not the user is using the iOS operating system or Android system.

Further, none of the Hong Kong-manufactured fitness bands that werer examined provided sufficient information on where the personal data would be stored, or whether third party vendors are used to help store the data. This was again consistent with the global results, where only 32% provided information on how a user's personal data was stored. But out of these 32%, only a few actually explained to users where their data was stored, the period of retention and the form in which their data was kept.

Despite the current climate of cyber attacks and data leaks, only one of the Hong Kong-manufactured fitness bands examined committed to users that it would employ security measures to safeguard their personal data. After further enquiries, the PC found that two out of the five local manufacturers did not encrypt the data whilst it was being stored and transmitted (note that two of the other local manufacturers did not respond to the PC's enquiries). In comparison, 51% of the global IoT devices examined provided information to users on how their personal data was being safeguarded.

The study also revealed that none of the local manufacturers informed users how they could delete their personal data collected by the fitness bands and related mobile apps – although one of the local manufacturers did provide users with an email address for the sending of data erasure requests. This is in line with the global results, where only 28% of the IoT devices reviewed provided such information to users.

Lastly, only two of the five local manufacturers provided contact details to users for them to submit any privacy-related queries and to exercise their data access and correction rights. This is lower than the global figure of 62%.

The Global Sweep clearly revealed a general lack of transparency and the potential collection of excessive data amongst IoT devices – or even possibly a lack of awareness by manufacturers of their obligations under data privacy laws.

Recommendations

The PC highlighted the need for further transparency and safeguards in relation to the handling of personal data by IoT devices. In particular, IoT devices (and their related mobile applications) should:

- Provide a privacy policy to users, which informs them in a clear and simple manner the types of personal data that will be collected, the purpose of collection, any potential transferees of the personal data, and the security safeguarding measures in place;

Data Privacy Cont'd

- Adopt privacy as the default position (i.e. "privacy by design") in order to minimise the excessive collection of personal data, including using default settings that are the least privacy intrusive;
- Implement security measures to protect personal data whilst it is being transmitted or stored;
- Explicitly inform users that they have the right to opt-out of the collection of data that is not relevant to the main function of the IoT device (e.g. phone book, etc);
- Provide clear instructions to users on how they can delete their personal data stored on the IoT device, the related mobile application and any backend servers; and
- Provide the data user's contact information to consumers so that they have a channel with which to submit any privacy-related queries or data access and correction requests.

Do not assume that a "one size fits all" approach will be sufficient, as this is usually not the case. A common mistake made by data users is to assume that they can simply use the same privacy policy on their website for their mobile applications. However, these privacy policies are usually not appropriate, as they do not specifically address and deal with the particular personal data being collected for the purposes of the mobile applications. Data users should also not forget about their notification obligations under data protection principle 1 of the PDPO, or the direct marketing restrictions.

These observations and recommendations are interesting. To a certain extent they do not move the discussion much further as they zoom into a small section of IoT, namely that of manufacturers of wearable technology devices. The more difficult question concerns the increase of connectivity of day-to-day experiences and the move towards smaller devices, with little or no user interface at all. How realistic in such a context is the fundamental principle of privacy law of notice and consent? How many times should consumers be asked to make decisions about their data given its almost ubiquitous collection?

The concerns surrounding wearable technology which relate to privacy and security cannot be underplayed. A bigger and very interesting conversation is just beginning.

CHINA

Technology

By Gabriela Kennedy, Partner, Mayer Brown JSM, Hong Kong
Xiaoyan Zhang, Counsel, Mayer Brown JSM, Shanghai

China Launches Internet App Store Registration Program

On 13 January 2017, the Cyberspace Administration of China ("**CAC**") announced the commencement on 16 January 2017 of the Internet app store registration program in China. The registration requirement was imposed by the mobile apps regulation that became effective in August last year. Specifically, Article 5 of the *Administrative Provisions on Information Services of Mobile Internet Application Programs* ("**Mobile Provisions**") requires Internet app stores in China to register with the local offices of the Cyberspace Administration within 30 days of the launch of business operations. "Internet apps stores" cover platforms on which various applications are provided for users to browse, search and download (such as iTunes, Google Play, Baidu Shouji, Tencent Myapp, and SnapPea), or the development tools and products released on the Internet (such as Apple Developer, Google Developers, and Xiaomi Developer).

Internet app stores need to: (i) apply for registration immediately upon the commencement of business operations; (ii) apply when any registration information needs to be updated; and (iii) communicate with the Cyberspace Administration when they terminate their business operations. Registrations shall be made locally where the store's ICP business license was obtained. Violations of the registration requirements are punishable though the actual offences/fines have yet to be stipulated.

Other than registration, an Internet app store is required to fulfil a long list of administrative responsibilities over its app providers pursuant to the Mobile Provisions: (i) verify the authenticity, security, legality of app providers and establish a credit management system; (ii) require app providers to protect users' information and provide a privacy notice to users; (iii) require app providers to improve their security review mechanism and appoint security personnel; (iv) require app providers to only release legitimate application programs, and respect the

Technology Cont'd

intellectual property rights of other app providers; (v) upon becoming aware of a violation, take measures such as issuing a warning, suspending the release or taking down the app as the case may be, and report the same to the relevant authorities; (vi) sign a service agreement with app providers and require them to comply with the laws, regulations and rules of the platform; and (vii) assist relevant authorities with any investigations, and assume public oversight by establishing channels and procedures for lodging complaints.

These requirements appear to be one of many efforts China has recently undertaken to crack down on malicious Internet apps by tightening control over app stores. "Malicious" apps refers to apps distributing content deemed to endanger national security, disrupt social order, or apps otherwise prohibited by Chinese laws, infringing users' legitimate rights, and/or containing serious security flaws. Some of the requirements in the Mobile Provisions are to be welcomed, such as IPR infringement and security issues while others which may be seen to equal a censorship requirement over app content may meet with less enthusiasm especially from foreign businesses operating in China. ◆

Contact Us

GABRIELA KENNEDY
Partner
+852 2843 2380
gabriela.kennedy@mayerbrownjsm.com

BENJAMIN CHOI
Partner
+852 2843 2555
benjamin.choi@mayerbrownjsm.com

ROSITA LI
Partner
+852 2843 4287
rosita.li@mayerbrownjsm.com

XIAOYAN ZHANG
Counsel (New York, USA)
+852 2843 2209
xiaoyan.zhang@mayerbrownjsm.com

AMITA KAUR HAYLOCK
Senior Associate
+852 2843 2579
amita.haylock@mayerbrownjsm.com

KAREN H.F. LEE
Senior Associate
+852 2843 4452
karen.hf.lee@mayerbrownjsm.com

Mayer Brown JSM is part of Mayer Brown, a global legal services organisation, advising many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, CAC 40, DAX, Hang Seng and Nikkei index companies and more than half of the world's largest banks. Our legal services include banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrownjsm.com for comprehensive contact information for all our offices.